FRONTEX
EUROPEAN BORDER AND COAST GUARD AGENCY

Warsaw, 25.01.2019

Handbook to the Operational Plan

Version January 2019

Joint Maritime Operations

Frontex - European Border and Coast Guard Agency
www.frontex.europa.eu | Pl. Europejski 6, 00-844 Warsaw, Poland | Tel. +48 22 205 95 00 | Fax +48 22 205 95 01

INDEX

Table of Contents

1. GUIDELINES FOR DEBRIEFING ACTIVITIES

1.1. Introduction

[redacted]

Commented [KB1]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and/or coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

1.2. Debriefing

[redacted]

1.3. Tasks of Debriefing Experts

[redacted]

1.3.1. Preparation for debriefing

[redacted]

[redacted]

Commented [KB2]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and/or coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

[redacted]

Commented [KB3]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and/or coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

1.3.3. Conducting debriefing sessions

[redacted]

[redacted]

Commented [KB4]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and/or coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

[redacted]

[redacted].

Commented [KB5]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and/or coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

1.3.4. Reporting

[redacted]

1.4. Use of Interpreters

[redacted]

Commented [KB6]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and/or coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

2. GUIDELINES FOR SCREENING ACTIVITIES

2.1. Introduction

A high number of persons cross the external borders of EU without being in possession of valid travel/identification document. Screening interviews are carried out to establish a presumed nationality, the interviews are mandatory and allow the host national authority to carry out its national registration procedures. Screening is the first step in any national identification process. Screening activities are performed by officers of a competent national authority of a MS as defined in the profile of a screening expert.

2.2. Screening

Screening in the field of irregular immigration means to establish an assumption on the nationality of an undocumented person having crossed, or having attempted to cross, an external border irregularly in view of registering the arrival of the person and returning the Third Country national to her/his country of origin when applicable.

Screening experts perform screening interviews at the request of the host MS authorities. The screening interviews carried out by deployed screening experts should, as a general rule, be performed in close cooperation with a screening expert from the host MS and assisted by an interpreter. To facilitate the screening, it is also advised that the age and the gender of the person to be interviewed is taken into account when appointing the screening expert and interpreter.

2.3. Tasks of Screening Experts

The screening expert assists/supports officers of the national authority to screen irregular migrants at reception and detention facilities in the operational area of the host MS in order to establish a presumed nationality. They must also refer vulnerable persons and persons in need of international protection, and unaccompanied minors to the national authority.

When necessary and if available the screening expert will work together with interpreters provided by the national authority or deployed by a MS.

[redacted]

2.4. Preparation for screening

[redacted]

Commented [KB7]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and/or coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

[redacted]

2.6. Conducting screening interviews

[redacted]

"Vulnerable persons*" refers to minors / unaccompanied minors, disabled people, elderly people, pregnant women or girls, single parents with minor children, victims of human trafficking, persons in need of international protection, persons with serious illnesses, persons with mental disorders, persons in need of medical assistance, victims of gender-based violence, victims of female genital mutilation, persons in distress at sea, persons who have been subjected to torture, rape or other serious forms of psychological, physical or sexual violence and other persons in a particularly vulnerable situation. Note that vulnerabilities can appear at any moment of the screening process.

[redacted]

Commented [KB8]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and/or coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

[redacted]

Commented [KB9]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and/or coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

2.7. Working as a team with Interpreters

[redacted]

2.8. Results of screening interviews

[redacted]

Commented [KW10]: The non-disclosed part contains detailed information related to reporting tools and methods used by law enforcement officials to conduct border control tasks and counter criminal activities. Its disclosure would jeopardize the implementation of ongoing and future operations, and thus facilitate irregular migration and trafficking in human beings as the effectiveness of law enforcement measures would be significantly reduced. As disclosing this information would undermine the protection of the public interest as regards public security, this part is not disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

3. GUIDELINES FOR FINGERPRINTING AND REGISTRATION

3.1. General information

In accordance with the EURODAC Regulation[3], irregular migrants and persons in need of international protection apprehended in connection with an irregular border crossing - except for minors under the age of 14 years - must provide their fingerprints.

Conditions and location for registration, including waiting areas, must ensure and respect dignity of the persons involved in the process and take into account vulnerabilities and their prioritization. Dignity, respect and non discrimination for the persons to be registered should always be observed during the process. Fingerprints and registration data of women and minors should preferably be taken by female officers, in line with cultural and age sensitive considerations.

The process led by the Host MS should focus in particular on systematic identification, registration and fingerprinting by the following steps:

[redacted]

The persons alleging a violation of their fundamental rights shall be informed of the procedure for reporting such FR violations, including the possibility to file a complaint with Frontex in accordance to the Annex on Complaints Mechanism of the Operational Plan. The potential asylum seekers will be informed of the procedure for launching an asylum application and shall be referred by the Registration and fingerprinting officer to the respective national authority.

3.2. Tasks of experts

Fingerprinting and registration activities shall be carried out according to the host MS's procedures, in close cooperation with the national experts and under the command and control of a Team leader, an officer assigned by the respective law enforcement authority of the host MS. They must also refer vulnerable persons and persons in need of international protection, and unaccompanied minors to the national authority.

The tasks can be structured as follows: 1) informing migrants; 2) procedures in case of refusal; 3) lawful use of force; 4) referral and 5) reporting.

Commented [KB11]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and/or coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

[3] *REGULATION (EU) No 603/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast).*

3.2.1. Informing of migrants

At the start of the fingerprinting process, experts must inform each person on the obligation to give fingerprints, the purpose for collecting the fingerprints and the manner in which fingerprints will be processed, as required by Article 29 of the EURODAC Regulation. Information should be provided in writing, and where necessary, orally - in simple terms and taking in consideration the gender, age and cultural considerations - in a language the person understands or is reasonably supposed to understand. The cultural mediators / interpreters can be used in case of the language barriers occur. In order to facilitate information process it is highly recommended that Host MS prepare relevant number of posters in the registration places.

3.2.2. Procedures in case of refusal

When persons refuse to provide their fingerprints, officers should carefully inquire about the reasons for their refusal, and provide additional easy-to-understand information in a language that they understand about why fingerprints are being taken. If possible, this should be done with the support of an interpreter if/ when required. The persons to be fingerprinted should be given effective opportunities to voluntarily comply with fingerprinting requirements, including the possibility to stop the process of fingerprinting, provide additional information answering their questions and concerns, and allow for questions from the persons and continue the process at a later stage, allowing for the opportunity to appear for fingerprinting a second time if necessary, once an informed decision has been taken.

Gender, age and cultural considerations should be always taken into account when further information is required in case of refusals to provide fingerprints.

3.2.3. Use of force

In case counselling and information is not successful, and if the Host MS does not consider, where other less coercive alternatives to detention cannot be applied effectively, the Host MS may consider resorting to use of force as a last resort in order to enable fingerprinting of migrants.

Use of force can be used only by the Host MS officers. If the officer of Host MS decides to do this, the migrant is informed that coercion may be used in order to take their fingerprints. The procedure for the use of force should include a clear explanation to the migrant of the steps the officer intends to take. If the migrant still refuses to cooperate, the officer may apply the minimum level of force required only if strictly necessary, lawful and proportionate to the aim pursued, with due respect to the integrity and dignity of the person concerned.

The officer should demonstrate that there was no other practicable alternative measure to using reasonable coercion. A case-by-case assessment should always be made of whether there is no such alternative, taking into account the specific circumstances and vulnerabilities of the person concerned.

However, vulnerable people, such as minors, victims of torture, sexual or gender-based violence and victims of serious crimes or traumatised people shall not be coerced into giving fingerprints.

The use of coercion must always be recorded and a record of the procedure be retained for as long as necessary in order to enable the person concerned to legally challenge the actions of the authority.

[redacted]

[redacted]

Commented [KB12]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and/or coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

3.2.5. Reporting

[redacted]

Commented [KW13]: The non-disclosed part contains detailed information related to reporting tools and methods used by law enforcement officials to conduct border control tasks and counter criminal activities. Its disclosure would jeopardize the implementation of ongoing and future operations, and thus facilitate irregular migration and trafficking in human beings as the effectiveness of law enforcement measures would be significantly reduced. As disclosing this information would undermine the protection of the public interest as regards public security, this part is not disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

3.3. Use of cultural mediators / interpreters

It is of outmost importance that the use of cultural mediators /interpreters participate in the informative sessions regarding the obligations to give fingerprints, the purpose for collecting the fingerprinting and the manner in which fingerprints will be processed.

Moreover, possible support of the cultural mediators /interpreters in the counselling of those refusing fingerprinting is recommended. In such cases where the refusals still remains, the cultural mediators/ interpreters may also be involved for the explanation of the procedures for the use of force with a clear explanation to the migrant of the steps the officer intends to take in order to compel cooperation.

3.4. Vulnerable groups

Special consideration should be given to the vulnerable persons.

"Vulnerable persons*" refers to minors / unaccompanied minors, disabled people, elderly people, pregnant women or girls, single parents with minor children, victims of human trafficking, persons in need of international protection, persons with serious illnesses, persons with mental disorders, persons in need of medical assistance, victims of gender-based violence, victims of female genital mutilation, persons in distress at sea, persons who have been subjected to torture, rape or other serious forms of psychological, physical or sexual violence and other persons in a particularly vulnerable situation. Note that vulnerabilities can appear at any moment of the screening process.

When the officers doubt about the age declared by the undocumented person to be registered (either when declaring that they are minors or an adults), the principle of presumption of minority should prevail and the situation should be immediately notified to the national authorities so that procedure for age determination can be started.

Use of force should not apply to vulnerable persons for the purpose of fingerprinting and other alternatives to seek cooperation for fingerprinting purposes should be sought, such as support from social services or organisations specialised in dealing with vulnerable persons.

4. REPORTING OF FRONTEX DOCUMENT ALERTS

4.1. Scope and Exclusions

This procedure refers solely to the reporting, validation and dissemination of Frontex Document Alerts (FDA).

The procedure applies to all Frontex personnel and participants involved in the reporting, validation and dissemination of FDAs related to any Frontex coordinated operational activities. FDAs may only be drafted and reported in conjunction with Frontex coordinated operational activities[4].

This procedure implements the existing methods of document alert reporting in Frontex, in line with the existing rules, procedures and provisions of the different Operational and/or Implementation Plans (air, land, sea), as agreed with the Host and Home Countries and other relevant participants[5].

This procedure does not apply to the thorough analysis of the reported information or to any risk analysis performed by the Frontex Risk Analysis Unit according to its own internal procedures and processes.

This procedure also does not apply to the incidents reported in JORA[6]. For that reporting the applicable JORA Policies and Procedures shall be followed.

4.2. Definitions and Classifications

4.2.1. Document and Identity Fraud

Following the definition established by the European Document Fraud Network (EDF), for the purpose of this SOP, document fraud shall mean any illegal use of an authentic document (by the means of impersonation or the use of fraudulently obtained genuine documents) as well as the use of forged, counterfeit, pseudo or stolen blank (and unlawfully personalized) documents.

In line with the above definition, for the purpose of this SOP identity fraud shall mean any illegal use of an authentic document or fraudulently/obtained authentic document [redacted]

Commented [KW14]: The non-disclosed part contains detailed information regarding the modus operandi of criminal networks involved in the smuggling and migrants and trafficking in human beings. Its disclosure would jeopardize the work of law enforcement officials and pose a hazard to the course of ongoing and future operations aimed at curtailing the activities of such networks, ultimately obstructing their purpose to counter and prevent cross-border crime as well as to prevent unauthorized border crossings. The disclosure would thus undermine the protection of the public interest as regards public security as laid down in Article 4(1)(a) first indent of Regulation (EC) 1049/2001.

4.2.2. Documents relevant for an FDA

For the purpose of this SOP, a document shall mean any piece of a written, printed, or electronic matter that provides information or evidence or that serves as an official record.

Any document that is subject to fraud in line with the above definitions may be relevant for reporting. In particular, all kinds of travel and identity documents, such as passports, ID cards, residence permits, visas, driving licenses, breeder documents and civil registration documents; border stamps; and registration documents of transportation means, their parts and machinery[8].

4 Member States and Third Countries may decide to inform Frontex about document fraud cases of high importance also out of the scope of Frontex coordinated operational activities. For that purpose, as a general rule, they use their own approved national document alert templates and they may decide to share these alerts with Frontex at the level of their national forgery desks. They may also decide to use the FDA template according to their convenience. Nevertheless, document alerts reported outside the scope of Frontex coordinated operational activities are not validated by Frontex.

5 Parallel with the implementation of this procedure CED is initiating an agency-wide discussion on a new concept of document fraud related information reporting. However, as long as a final agreement is not reached, that discussion shall have no impact on the implementation of this procedure. CED is responsible to update this procedure as soon as a new document alert reporting concept has been agreed in Frontex.

6 Joint Operations Reporting Application - for reference consult the respective part of the Handbook to the Operational Plan.

[redacted]

8 Note, it is impossible to provide an explicit list of documents that are relevant for FDA reporting due to the fact that the recognition of travel, identity or registration documents is a merit of national sovereignty and it is governed by different national laws and rules in each Member State. Nevertheless, there is a definition provided to travel and identity documents in Chapter 4.6

4.2.3. Frontex Document Alert (FDA)

The Frontex Document Alert is a duly-compiled template reporting a document or identity fraud case detected in the context of Frontex coordinated operational activities.

FDAs shall be completed in English only and shall contain no personal data.

The FDA has three categories as described in the chapter 4.2.4 below. A template copy of each category is available in chapter 15.

4.2.4. Categories of Frontex Document Alerts

Frontex Document Alerts are catalogued into three main categories. Each category has its own template available in chapter 15.

[redacted]

Commented [KB15]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and/or coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

4.2.5. Cases to be reported in a Frontex Document Alert

Cases of interest reported in an FDA shall meet at least one of the following conditions:

[redacted]

In order to determine the existence of the aforementioned conditions, the FDA initiator shall consult the local case handler or the representative officer of the Host Country, check existing alerts and databases and assess the case using their personal experience, knowledge and skills (expert judgement).

[redacted]

[10] *CIRAM version 2.0.*

[11] *CIRAM version 2.0.*

4.2.6. Relevant Frontex Activities

FDAs are reported in Frontex coordinated Joint Operations, Pilot Projects, Rapid Interventions and deployment of Migration Management Support Teams.

Frontex actively participates in the implementation of the EMPACT Policy Cycle, and in particular in the implementation of respective EMPACT Operational Actions (OA) and Joint Action Days (JAD). It remains in the sole responsibility of the respective action leaders to decide whether in their respective action the use of the FDA reporting structure is suitable. In case of need the FDA templates may be used during EMPACT actions and may be processed in line with the provisions of chapter 4.5 (Procedure and process flow).

4.2.7. Other relevant definitions and terminology

The main common terms and descriptions used in the environment of document and identity fraud, listed in iFADO12 and other important sources, are set out in chapter 4.6.

4.3. FDA HelpDesk

The CED is responsible to set up and maintain the FDA HelpDesk. [redacted] The contact details of the FDA HelpDesk are included in the respective annex of the Operational Plans.

The FDA HelpDesk can only be contacted concerning cases that are, or are going to be, reported as an FDA. Any other requests will not be dealt with by CED but may be referred to the competent Frontex entity[13].

Commented [KW16]: The non-disclosed part contains detailed information on the means of communication used by law enforcement officials. The disclosure of this information would put law enforcement officials' work in jeopardy and harm the course of future and ongoing operations aimed at curtailing the activities of organized criminal networks involved in the smuggling and migrants and trafficking in human beings. As the disclosure of such pieces of information would undermine the protection of the public interest as regards public security, it must therefore be refused as laid down in Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and/or coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

The non-disclosed parts contain information regarding the number and profiles of officers deployed in the operational area. Disclosing such information would be tantamount to disclosing the weaknesses and strengths of Frontex operations and pose a risk to their effectiveness. As a result, the course of ongoing and future similar operations would be hampered, ultimately defeating their purpose to counter and prevent cross-border crime and unauthorized border crossings. Consequently, the disclosure of such information would undermine the protection of the public interest as regards public security as laid down Article 4(1)(a) first indent of Regulation (EC) 1049/2001.

4.4. Roles and Responsibilities

4.4.1. Local Case Handler

The local case handler is a public or law enforcement officer of the Host Country assigned at the place of detection. The local case handler is the authorised person at the place of detection for the processing of the detected case in line with the procedures, rules and regulations applicable in the Host Country.

4.4.2. FDA Initiator

An FDA Initiator is a Frontex Team Member, Seconded Team Member or any Host Country representative who matches any one of the following Frontex profiles[14]:

[redacted]

[12] *Intranet False and Authentic Documents Online portal of the General Secretariat of the Council of the EU - http://www.consilium.europa.eu/en/ifado/ifadocontacts.htm*

[13] *In case of queries where Frontex has no competence to act, the caller will be informed accordingly.*

[14] *Established in Management Board Decision 38/2016 of 23 November 2016 adopting the profiles and the overall number of border guards and other relevant staff to be made available to the European Border and Coast Guard teams.*

If there are no officers available with the above profiles in the place of detection, exceptionally any other officer of a host and participating MS (e.g. debriefing expert, screening expert) may act as a FDA initiator, provided that he/she has technical expertise and skills to report document or identity fraud.

Document experts (TAs and/or SNEs) of Frontex CED may also act as FDA initiators when deployed to operational missions in Frontex coordinated operational activities. No other regular staff member of Frontex may act as FDA initiator, except in case he/she matches one of the above profiles and he/she is authorized in written by the Head of Frontex CED to act as FDA initiator.

The local case handler may also act as an FDA Initiator and carry out the same functions as long as the requirements for such role are met as subsequently illustrated. In order to complete the assigned task, the local case handler may request the support of any Frontex deployed team member who meets the requirements to act as an FDA Initiator.

Third Country Observers involved in Frontex coordinated operational activities may also act as an FDA Initiator provided that they match the conditions of the above profiles and are requested by a representative of the Host Country to act (under instructions from and in the presence of the relevant officer of the Host MS).

The FDA Initiator is responsible to compile the FDA template in reference to a case of interest indicated in chapter 4.2.5, adhering to the following initial guidelines.

[redacted]

Commented [KB17]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and/or coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

The non-disclosed part contains detailed information on the means of communication used by law enforcement officials. The disclosure of this information would put law enforcement officials' work in jeopardy and harm the course of future and ongoing operations aimed at curtailing the activities of organized criminal networks involved in the smuggling and migrants and trafficking in human beings. As the disclosure of such pieces of information would undermine the protection of the public interest as regards public security, it must therefore be refused as laid down in Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

4.4.3. FDA Validator

The FDA Validator is a Document Expert (TA or SNE) from the Operational Support Team of Frontex CED. The FDA Validator may not validate FDA in cases where he/she has been the original FDA Initiator.

4.4.4. FDA HelpDesk Duty Officer

The FDA HelpDesk Duty Officer is a Document Expert of CED to whom the FDA Service phone has been assigned and who is responsible to monitor both the service phone and the FDA mailbox and respond to any quires in line with this SOPs.

[redacted] He/she is also responsible to call back any caller who was trying to reach the service phone after working hours.

[redacted]

4.5. Procedure and Process Flow

Participants in relevant Frontex activities (as described in chapter 4.2.6) have the obligation to report an FDA in a timely manner once a case of interest (as described in chapter 4.2.5) has been detected and verified.

The FDA Initiator will consequently compile the FDA template and send it to the designated recipient mailbox - [redacted] copying the email address of the respective operational team and the relevant official email addresses of the Host Country.

The FDA will then be registered by one Document Alert Validator, checked and forwarded to the higher level for a final acceptance.

The endorsed FDA will then be uploaded onto FOSS and other dispensed FRONTEX digital platforms.

4.5.1. Frontex Document Alert Reporting

Complementing the guidelines provided in chapter 4.4.2, the technical instructions hereunder should be completed by the FDA initiator in order to submit the FDA for the subsequent validation procedure.

4.5.2. General Information

[redacted]

4.5.3. FDA Header

[redacted]

[redacted]

Commented [KB18]: The non-disclosed part contains detailed information on the means of communication used by law enforcement officials. The disclosure of this information would put law enforcement officials' work in jeopardy and harm the course of future and ongoing operations aimed at curtailing the activities of organized criminal networks involved in the smuggling and migrants and trafficking in human beings. As the disclosure of such pieces of information would undermine the protection of the public interest as regards public security, it must therefore be refused as laid down in Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

Commented [KB19]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and/or coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

[redacted]

4.5.4. FDA Main Part:

[redacted]

Commented [KB20]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and/or coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

4.5.5. Frontex FDA assignment for validation

[redacted]

Commented [KW21]: The non-disclosed part contains detailed information on the means of communication used by law enforcement officials. The disclosure of this information would put law enforcement officials' work in jeopardy and harm the course of future and ongoing operations aimed at curtailing the activities of organized criminal networks involved in the smuggling and migrants and trafficking in human beings. As the disclosure of such pieces of information would undermine the protection of the public interest as regards public security, it must therefore be refused as laid down in Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

[redacted]

4.5.6. Frontex FDA finalization

[redacted]

Commented [KB22]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and/or coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

4.6. Other relevant definitions and terminology

Travel documents[22]: a passport or other equivalent document entitling the holder to cross the external borders and to which a visa may be affixed[23];

ID documents: documents used to identify its holder and issuer, which may carry data required as input for the intended use of the document[24];

Breeder documents: The issuing of passports in the Member States of the EU is dealt with under the national law of those Member States. National law requires presentation of various documents, such as a birth certificate, citizenship certificate, family book, parental authorization, driving license, utility bill, etc. These documents are usually called 'breeder' documents, as passports may stem from them[25];

Forged document: a previously authentic, lawfully issued document that has since been altered (falsified) by an unauthorised agent. This category includes several types of forgeries.

Counterfeit document: An unissued document, an unauthorised copy or reproduction of a document (documents entirely produced by a forger)[26];

Impostor: A person who practices deception under an assumed character, identity or name;

Pseudo document: has the appearance of an official document, but is not issued by a legally recognized, existing authority or institution of a State or Organisation recognised under International Law, and so has no legal validity. This category also includes:

Fantasy document: referred to imaginary states or organisations. The issuer is neither a state recognised under international law nor an authorized institution.

Camouflage document: claim to come from countries or organisations that no longer exist or have a new name.

Other pseudo document: other types of document that bear the name of an existing state or organization but do not correspond to any existing real document in the country or international organization indicated (sometimes also called fictitious documents).

[redacted]

[22] *As the recognition of travel documents is solely a national competence, the following databases of the Council of the EU may be consulted to determine what documents are recognised in which Member State to cross the external borders. Concerning documents of EU Member States: h://www.consilium.europa.eu/prado/en/prado-recognised-documents.html; for Third Countries: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/borders-and-visas/document-security/docs/part_i_travel_documents_issued_by_third_countries_and_territorial_entities_en.xlsx*

[23] *Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), chapter 4.7*

[24] *ICAO, Document 9303, (7th edition, 2015), Page 13*

[25] *Opinion of the European Data Protection Supervisor no. 2008/C 200/01; Official Journal of the European Union 2008/C200/1*

[26] *From b) to h). Definitions from General Secretariat of the Council of the EU, "Glossary of Security Documents, Security Features and other related technical terms (FADO glossary)", (2013)*

Documents Stolen in Blank: An unissued, authentic document blank has been misappropriated and personalized by an unauthorized person (by a forger).

Fraudulently obtained authentic/genuine travel documents: This term covers both authentic documents applied for on the basis of fraudulent source documents, as well as fraudulently issued authentic;

Fraudulently obtained authentic/genuine travel documents: Infiltration at the stage of enrolment through submission of a morphed image to the document issuing authority to obtain a genuine ID or travel document;

Genuine/Authentic documents: A document issued by a recognized, authorized and competent authority, itself not altered in any way (RAU-EDF 2015);

Face/Image Morphing: blending two or more facial images into one with the assistance of digital programs[27].

Type of Presentation Attack: defined as the "presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system" (ISO/IEC 30107-1:2016);

Biometric Presentation Attack: the use of an artificial object (morphed image) that mimics characteristics of a valid biometric in order to subvert a biometric system, i.e. evade passport border controls or cause missed identification in a watch list.

[redacted]

[redacted]

4.7. Protection of Personal Data in images

[redacted]

Commented [KB23]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and/or coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

[27] *COM(2016) 790 final, Action plan to strengthen the European response to travel document fraud*

[redacted]

Commented [KB24]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and/or coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

[redacted]

Commented [KB25]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and/or coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

[redacted]

[redacted]

[redacted]

Commented [KB26]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and/or coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

4.8. Travel and ID Documents Alert file naming conventions

[redacted]

[redacted]

Commented [KB27]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and/or coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

5. REFERENCES TO THE EUROPEAN COOPERATION ON COAST GUARD FUNCTIONS WITHIN JOINT OPERATIONS AND OTHER TAILORED ACTIVITIES

5.1. Legal and operational framework

On 6 October 2016 new amendments to the legal frameworks of the European Maritime Safety Agency (EMSA), European Fisheries Control Agency (EFCA) and European Border and Coast Guard Agency (Frontex) entered into the force setting additional tasks and responsibilities for the Agency in relation to coast guard functions[28] within European Border and Coast Guard Regulation (thereafter - Regulation), particularly:

- Art. 4: European Integrated Border Management was introduced within the Regulation and has been upgraded by adding additional/new elements including - SAR;
- Art. 8: Frontex shall provide technical and operational assistance to Member States and third countries in accordance with Regulation (EU) No 656/2014 and international law, in support of search and rescue operations for persons in distress at sea which may arise during border surveillance operations at sea;
- Art. 15 para 5: The objectives of a joint operation or rapid border intervention may be achieved as part of a multipurpose operation. Such operations may involve coast guard functions and the prevention of cross-border crime, including the fight against migrant smuggling or trafficking in human beings, and migration management, including identification, registration, debriefing and return.
- Art. 53: Frontex, in cooperation with the European Fisheries Control Agency (EFCA) and the European Maritime Safety Agency (EMSA), will provide support to national authorities carrying out coast guard functions at national and EU level and, where appropriate, at international level.
- Art. 81(c): Depicts the mechanism set to evaluate the Agency, among other, on the implementation of European cooperation on coast guard functions.

Respective Coast Guard functions and law enforcement related activities are incorporated in Frontex joint operations in the field leading to operationalization of the European cooperation on coast guard functions and fight against cross-border crime, in particular maritime safety, security, search and rescue, fisheries control, customs control, general law enforcement and environmental protection, in accordance with the EUROSUR objectives, European Integrated Border Management and European Maritime Security Strategy.

As regards strategic elements Agencies agreed [29] :

- To set up an annual European Coast Guard event[30] with involvement of national authorities performing coast guard functions and other EU and international partners for consultation and feedback on Agencies' cooperation activities.
- To implement technical subcommittees to support the implementation of the Annual Strategic Plan[31].
- To identify of new areas of mutual interest for interagency cooperation including new or amendment of existing Memoranda of Understanding (MoUs)/Service Level Agreements (SLAs).
- To increase coordination of the Agencies' communication activities related to the implementation of the interagency cooperation on coast guard functions.

---

[28] Maritime safety, security, search and rescue, border control, fisheries control, customs control, general law enforcement and environmental protection.

[29] Tripartite Working Arrangement (TWA) signed in March 2017 which was approved by EMSA, EFCA and Frontex governing boards and entered into force on 17 March 2017 after three EDs signed it. The TWA forms the legal basis and describes more in detailed the governance and sets strategic areas of cooperation among the Agencies. Regulation (EU) 2016/1624, Regulation (EU) 2016/1625 and Regulation (EU) 2016/1626 of the European Parliament and of the Council of 14 September 2016.

[30] The 1st event was organized in Vigo on 11 and 12 April 2018.

[31] TSC1 (Sharing of information and surveillance services); TSC2 (Capacity building and risk assessment); TSC3 (Sharing capacity and legal issues).

The permanent Frontex maritime JO in Mediterranean Sea are, by priority, the operational platform for implementation of European Coast Guard functions.

Tailored activities related to Coast Guard functions could be implemented whenever there is an operational need and even if Frontex maritime JO are not implemented (e.g. the Baltic Sea, the Black Sea, etc.).

5.2. Enhanced cooperation in the frame of the Coast Guard Functions

The purpose of this paragraph on Coast Guard functions is to define a common approach at Agencies level on activities implemented at maritime domain in order to improve co-operation and co-ordination between the relevant Member States' authorities, EU Agencies and other bodies performing coast guard functions.

Frontex in cooperation with EFCA and the EMSA, will provide support to national authorities carrying out coast guard functions at national and EU level and, where appropriate, at international level, as defined in the Art. 53 of the Regulation, in particular:

- Sharing, fusing and analysing information;
- Providing surveillance and communication services;
- Building capacity (guidelines, recommendations, best practices, training and exchange of staff);
- Enhancing the exchange of information and cooperation;
- Sharing capacity by planning and implementing multipurpose operations.

In this frame, Frontex, EFCA and EMSA will particularly develop cooperation on:

- Sharing capacity (e.g. providing possibilities to other EFCA and EMSA to foster implementation of their tasks while not deviating from the core Frontex tasks);
- Exchange of patrolling schedules (periodic information exchange by operational actors as minimum once a month and if there is an operational need on more frequent basis);
- Operational briefings (usually done at ICC level and organized on periodic basis depending on staff rotation and availability of the experts from the Agency);
- Reporting and registering sighting information (reporting in a standardized way on commonly agreed objects of interest for EFCA and EMSA);
- Participating in thematic workshops/meetings (to support with specific input to other Agencies in relation to meetings on CG functions);
- Deploying specific Coast Guard expert such as European Coast Guard Functions Officer (EUCGFO) for the benefit of the 3 Agencies and the Member State concerned and being able to properly fulfil its tasks taking in consideration, the full spectrum of the Coast Guard Functions implemented in the frame of the Frontex JO involving the concerned competent national authorities
- Any other mutual cooperation modalities could be agreed on case by cases basis (e.g. production of CONOPS, handbook, etc.).

6. LAW ENFORCEMENT FUNCTIONS WITHIN JOINT OPERATIONS

6.1. Legal and operational framework

According to the Regulation, the Agency has received new competences and tasks as regards law enforcement functions, mainly related to cross-border crime and terrorism. In accordance with the Frontex mandate, which came into force as of 6 October 2016, the Agency is entitled to have an enhanced focus on the co-operation of border authorities and the joint efforts to effectively counteract cross-border crime, including illegal immigration, trafficking in human beings, the smuggling of drugs and excise goods, trafficking of firearms and terrorism.

The enhanced mandate of the Agency in conjunction with the given objectives to contribute to preventing and detecting serious crime with a cross-border dimension in accordance with the corresponding definitions is asked to collaborate with EUROPOL and EUROJUST, other relevant EU agencies and bodies, EU MS' national services, law enforcement and border management authorities, as well as relevant international organizations and regional cooperation networks.

By expanding its tasks, the Regulation now allows Frontex to […]

- *"**contribute to preventing and detecting serious crime with a cross-border dimension**, such as migrant smuggling, trafficking in human beings and terrorism, where it is appropriate for it to act and where it has obtained relevant information through its activities."*
- […]-*"organise the appropriate technical and operational assistance to Member States so as to reinforce their capacity to implement their obligations with regard to the control of the external borders and to face challenges at the external borders resulting from illegal immigration or **cross-border crime**. Such assistance should be without prejudice to the relevant national authorities' competence to initiate criminal investigations"*.
- contribute to […] *"addressing serious crime with **a cross-border dimension**, to ensure a high level of internal security within the Union."*. The Regulation also defines cross-border crime as *"any serious crime with a cross-border dimension committed at or along, or which is related to, the external borders."*

According to Article 8(1)(m) of the Regulation, Frontex cooperates with Europol and Eurojust within respective mandates of the agencies concerned, and provides support to Member States in circumstances requiring increased technical and operational assistance at the external borders in the fight against organised cross-border crime and terrorism;

This specific support may be granted by EMPACT/EU Policy Cycle Operational Actions platform. EMPACT is an ad hoc management environment to develop activities in order to achieve pre-set goals. It is a structured multidisciplinary co-operation platform of the relevant Member States, EU institutions and agencies, as well as third countries, international organisations and other (public and private) partners to address the prioritised threats of organised and serious international crime[32]. This support can also be provided in alignment with current Joint Operations.

6.2. Enhanced cooperation in the frame of the Law Enforcement Functions

Within its mandate, Frontex contributes to preventing and detecting serious crime with a cross-border dimension. It also collaborates with EUROPOL and EUROJUST and other relevant EU agencies and bodies, EU MS' law enforcement and border management authorities, as well as relevant international organizations and respective regional cooperation networks.

Frontex activities initiated and coordinated by the Coast Guard and Law Enforcement Unit and its Law Enforcement Sector contribute to the fight against cross-border crime in maritime JOs by:

[32] *As defined on Europol website: https://www.europol.europa.eu/*

- Promotion and facilitation of cooperation of law enforcement authorities responsible for pre-investigative activities, investigation and prosecution of border related criminal activities within the EU MS, as well as with Third Countries.
- Operationalization of working processes and entail in bridging border guard, police and customs authorities as well as other bodies responsible for border management and law enforcement, with the aim to counteract various types of cross-border crime and terrorism related threats.
- Initiating and implementing law enforcement related activities in the frame of the EU Policy Cycle/EMPACT operational activities. To further contribute to the EU fight against serious and organized crime by participating in the strategic planning supporting relevant actions, and to coordinate Joint Action Days (JADs).
- Implementing the Investigation Support Activities related to Cross-Border Crime (ISA-CBC)[33] by developing the concept of the investigation support activities aligned with the objectives under EU Policy Cycle and complementing the multi-purpose JOs. The investigation support activities will serve the purpose of enhanced operational cooperation of border and coast guard and the criminal police/investigative units, as well as customs authorities when needed. It will be co-organized in close cooperation with EU MS based on their consent.
- Supporting regional cooperation networks and EU CSDP missions and operations related to cross-border crime prevention and detection and to enhance the operational cooperation of law enforcement and border control authorities.
- Advising, supporting and contributing to planning and implementing Frontex Operational Plans, with a focus on operational results.
- Harmonizing law enforcement cooperation by designing adequate modules into Multipurpose Joint Operations, EURTF/Hotspots, Coordination/Contact Points concepts, Flexible Operational Activities, operational pilot projects and other cross-border crime related actions.
- Supporting maritime JOs applying the EMPACT related activities in order to better prevent and detect cross-border crime.
- Supporting maritime JOs by contributing to the dismantling of organized crime groups active in the area of Environmental crime (e.g. maritime pollution, dumping of waste and other harmful substances, illicit waste trafficking). The involvement in Environmental Crime EMPACT Priority will allow to combine the coast guard and law enforcement functions simultaneously.

[33] *Pilot Project approved by the Executive Director of Frontex on the 10th of September 2018.*

7. HOTSPOTS AND EU REGIONAL TASK FORCE

7.1. General information

Hotspot area means an area in which the host MS, the Commission, relevant Union agencies and participating Member States cooperate, with the aim of managing an existing or potential disproportionate migratory challenge characterised by a significant increase in the number of migrants arriving at the external borders.

At hotspot areas Migration management support teams (MMST) can be deployed which provide technical and operational reinforcement to MS and which is composed of experts deployed from MS by the Frontex, EASO, Europol or other relevant Union agencies.

The European Union Regional Task Force (EURTF) represents the platform for implementing the Hotspots concept and provides overall operational coordination of the work of different teams of experts from the EU Agencies involved, facilitates and manages the information exchange among these teams, and it supports the coordination of its operational efforts with the relevant national authorities.

The implementation of the "hotspots" concept in the scope of Frontex mandate is integrated within the framework of the respective Frontex coordinated joint operation. Frontex supports the host MS in implementation of the following activities, in particular:

- Assistance in identification including nationality screening,
- Referral of people in need of international protection,
- Assistance in registration including fingerprinting, which precedes the asylum applications.

In addition, Frontex s supports the host MS in organizing of adequate return assistance with regard to persons upon who's the competent national authorities have issued a return decision.

7.2. Roles of EU Agencies

Frontex, European Asylum Support Office (EASO), Europol and Eurojust provide operational assistance to the MS in accordance with their respective mandate in the field of managing the external borders, dealing with applications for international protection, and combatting serious organized crime such as facilitation of irregular migration

Frontex supports MS in the identification procedures through screening, debriefing, fingerprinting collection and document expertise. Moreover, Frontex provides tailored products and services within the context of Eurosur.

The concept of the "Hotspot" foresees that the EASO, Frontex and Europol work on the established hotspots in the operational area to process incoming migrants by coordinating activities and complementing each other. Frontex assists MS in identification including nationality screening, registration and fingerprinting, which precedes the asylum applications. Those claiming asylum are immediately channelled into an asylum procedure where EASO support teams help to process asylum cases as quickly as possible. For those not filing a claim for international protection, Frontex helps MS by coordinating the return of irregular migrants. Europol and Eurojust assist the host MS with investigations to dismantle the smuggling and trafficking networks.

The EURTF, in close coordination and cooperation with the competent national authorities, facilitate the overall coordination of the teams of experts from the different Agencies deployed on the hotspots, and ensure information exchange. Depending on whether the major challenge is pressure at the external borders, or processing asylum applications or investigating criminal networks, the relevant Agency takes up the role of coordinator in the EURTF in cooperation with the competent authority of the host MS. Frontex take care of the administrative and logistical arrangements in cooperation with the competent authority of the host MS. The EURTF shall carry out its tasks without prejudice of the competences and responsibilities of the relevant national authorities, and in close collaboration with them.

The operational support to be provided using the "Hotspot" includes:

- Registration and screening of irregular migrants to determine their identity and assumed nationality, and provision of information concerning the asylum process and referral, in case of need. Fingerprinting and registration in EURODAC is carried out by host MS authorities, and if requested with the support the TM. At this stage, each individual undergoes a first screening interview. Following the screening it should be possible to distinguish between the following categories of persons:
    - Persons who wish to apply for asylum (actors: national competent authorities with the support of EASO);
    - Persons who can be subject to a return procedure in accordance with the EU law (actors: national competent authority with the support of Frontex);
    - Persons with regard to whom the situation may remain doubtful: normal procedure applies (actor: national competent authorities).

[redacted]

- Stepping up investigations (including forensic/operational support), information and intelligence exchange on facilitation of irregular transit and stay within the EU. This enhanced cooperation should deal with criminal networks facilitating migration to the EU as well as secondary movements from the MS of disembarkation to the final destination (Actors: host MS, in particular national prosecutors and judicial authorities, Europol, Eurojust, if needed).
- Asylum support and referral (if necessary), in line with the joint processing concept, by channelling asylum seekers into the appropriate asylum procedure (according to the Host MS national legal system) and assisting with registration of asylum seekers and subsequent preparation of case files.
- Coordination of the return of migrants that do not have the right to stay in the EU legally, in particular with regard to pre-return assistance and the coordination of return flights. Support for the acquisition of travel documents from countries of origin, including by setting up teams from identified countries of return to carry out interviews and speed-up the issuance of travel documents (Actors: host MS and other MS, which can assist in the contacts with the relevant countries of origin or transit with the support of Frontex).
- Interpretation to facilitate the work of the experts provided by the Agencies for the above tasks is provided by the Agencies and/or MS.

Commented [KW28]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

8. FRONTEX ONE-STOP-SHOP (FOSS)

Commented [KB29]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and/or coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

8.1. FOSS general information

[redacted]

8.2. FOSS access procedures

FOSS users are divided into "User Groups", with each group being granted a specific access level enabling its members to view or upload information, depending on their specific operational need.

[redacted]

8.2.1. FOSS access authorization

Access to FOSS is granted if the requestor meets the following conditions: has an operational need, provides the required user information and is authorized by the relevant authority.

[redacted]

8.2.1.1. Access authorization procedure for TM via OPERA:

When OPERA[34] is used the process of requesting and authorizing access to FOSS is fully performed through this system, by completing the section **"Additional information"**, under the **"Personal registration"** form in the **"Resources Deployment Tool"** page.

[redacted]

[34] *The Operational resources management system (Opera: https://fis.frontex.europa.eu/opera/) is an integrated system for the management of the operational resources pooled and deployed in Frontex coordinated activities.*

[redacted]

[redacted]

"**Type of Access**", by selecting one the following options:

- Standard overview of JO documents
- Full overview of JO documents
- Full sector overview

[redacted]

8.2.1.2. Access authorization procedure for TM (seconded):

- For TM (seconded) the same FOSS access procedures as for Frontex staff apply. Unless otherwise requested by the Operational Manager, the TM (seconded) is granted FOSS access to the relevant content on FOSS for the duration of the secondment through their Frontex email.

- Following the end of the secondment at Frontex the user's access to relevant FOSS section will be deactivated.

8.2.1.3. Access authorization procedure for the other participants (not inserted in OPERA):

- In the "FOSS User Access Request Form" the NFPOC approves the access request for their personnel deployed to the operation or other parties, by ticking one of the relevant boxes displayed in the form and identifying the joint operation to be accessed.
- The NFPOC sends the duly completed "FOSS User Access Request Form" to FOSS Administrator.
- The Operational Manager in liaison with ODSO approves the request and sends the relevant data back to the FOSS Administrator, in order to grant access.

Commented [KB30]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and/or coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

[redacted]

8.3. Roles & Responsibilities

8.3.1. National FOSS User Coordinator

This function is assigned to the relevant MS's NFPOC. The responsibilities include gathering user data, validating access and providing user data to the "Area of Interest Owner".

8.3.2. Area of Interest Owner

This function is assigned to the Operational Manager in charge of the Joint Operation. The responsibilities include establishing the structural design and layout of the specific section in the application (FOSS Area of Interest), uploading content in the specific section, authorizing user groups and permissions levels, providing all necessary information to the User Administrator.

8.3.3. FOSS Administrator

This function is assigned to the relevant contact person dealing with the FOSS matters. The responsibilities include creating, updating, removing and deactivating user accounts, assigning users to a respective group, assigning groups to the specific area of interest as well as other webmaster tasks related to content management and system administration.

8.4. Navigation in FOSS

After logging into FOSS, by scrolling on the section 'Operational Activities' authorized users will be able to access the relevant page, directly from the FOSS homepage. As an example, in the images below the user has been granted access rights to JO Focal Points Sea 2014:

Commented [KB31]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and/or coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

The user can also access the Operational Activities section, either from the left hand side menu, or from the central pane.

9. COMMUNICATION WITH THE PRESS

9.1. Introduction

All Frontex activities are financed from public funds (EU budget) therefore it is Frontex's obligation to maintain a high level of transparency and openness in its activities. Operations held at the external borders experiencing a high level of migratory pressure often draw a large numbers of international journalists.

It is Frontex policy to facilitate media coverage of all its activities, including operations with due respect for human dignity, privacy and protection of personal data. Consequently the press office facilitates media visits to the operational areas, including participation of media representatives in patrols and organises media interviews with officers deployed by Frontex.

All press visits are closely coordinated with host MS authorities and are carried out according to procedures defined in the Press Communication Rules in the sub-chapter below.

Press rules may vary depending on the operation; therefore the differences will be reflected in the main part of the Operational Plan.

In some operations Field Press Coordinators seconded from MS will be deployed to host MS to coordinate press requests in the field.

Openness cannot hinder or jeopardise operational activities, nor can it affect human dignity, therefore several general rules apply. Journalists should, for example, be prohibited to take pictures of migrants and refugees that could lead to their identification without their consent as this might put them in danger.

No information should be released to the media prior to the beginning of the operation.

Operational details, such as operational area, details of technical equipment deployed, shift schedule, etc. are considered sensitive information and are not to be shared with the media.

All participants in the joint operation are obliged to contact the Frontex Press Office before giving an interview.

9.2. Press communication rules

9.2.1. General

The communication strategy regarding the Frontex mission and activities in general is under the auspices of the Agency.

In order not to jeopardise the outcome of the operation, no information about the operation should be released to the public prior to its beginning. National authorities deploying border guards to the joint operation should also limit their public statements to the general objectives of the operation, numbers and profiles of experts.

Press Offices of Frontex and the host country are entirely responsible for coordination of all matters related to interview requests, press visits to the operational area and any other press-related matters related to the joint operation.

Press lines regarding joint border control operational issues and actions as well as specific incidents that might occur, are agreed by Frontex and the host country Press Office.

9.2.2. Tasks of press offices in the context of Joint Operations

Press visits to the joint operation will be organised by the host MS authorities in cooperation with the Frontex Press Office.

Tasks of the Frontex Press Office will include:

- Informing the media on Frontex' mission and activities, as well as on the activities of the Joint Operation. Providing background information and statistical data on migratory movements.
- Being the point of contact for international media requests.
- Media monitoring and analysis of media tendencies (neutral, positive, negative).
- Drafting and distributing press releases, statements and other communications in close cooperation with the competent host country authorities.

Tasks of the Host Country press office

- Arranging interviews with representatives of the host MS authorities.
- Being the point of contact for national media.
- Arranging filming opportunities in the operational area
- Drafting and distributing press releases, statements and other communications related to Frontex' activities in close cooperation with Frontex
- Informing Frontex Press Office about questions from national media regarding the Agency and its activities

9.2.3. Management of Press Requests

Given that journalists need to obtain authorisation from the host MS authorities to visit the operational area, the following procedures must be followed:

- Individual and on-the-spot media requests must be directed to the Frontex Press Office and press office in the host MS electronically.
- The Frontex Press Office and the press office from the host MS will inform each other about media requests on a regular basis.
- The Frontex Press Office will coordinate the flow of international press requests received, collect information about their needs and direct requests to the press office in the host MS.
- The press office of the host MS will process the necessary authorisations, coordinate the flow of national press requests received and inform the Frontex Press Office about the planned presence of the media in the operational area and provide them with necessary assistance on the ground.
- The press office of the host MS will process the necessary authorisations for participation of journalists in patrols and visits to restricted operational areas. The Dedicated Press Officer will inform the interested parties and the Frontex Press Office about the decision.
- The press office of the host MS will host media representatives. Media representatives will be asked to present their press credentials before participating in any activity and to sign a written statement that the host MS or other involved countries' authorities will not bear any responsibility should anything happen to the media representatives and/or their equipment.
- The press office of the MS which deploys the TM needs to be informed and approve the press request

9.2.4. Specific guidelines for participating officers if approached by the media:

Participants are allowed to talk to the media only within the limits set by specific guidelines indicated below.

All participants need to contact the Frontex Press Office before agreeing to an interview.

The Press Office will brief the TM prior to the interview about the media, subject of the interview and sensitive topics.

[redacted]

[redacted]

Commented [KB32]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and/or coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

[redacted]

- [redacted]

Please refer journalists to Frontex Spokesperson for further details or call the Frontex Press Office in case of doubt (you can also send an SMS and we will call you back).

Commented [KB33]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and/or coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

9.2.5. Contact details

The contact details of the Frontex Press Office members (Spokesperson and Press Officer) and the Press Office of the National Authority of the Host MS are indicated in the respective Annex of the Operational Plan "Contact Details".

10. JORA

10.1. JORA General Information

10.1.1. JORA product & service management

[redacted] The Product and Service Managers are listed in the JORA Actors Specific Annex.

The Product and Service Managers primary role is to ensure that the system runs properly, in line with the end-users needs and, if necessary, to manage the further developments or readjustments of the system.

The Product and Service Managers also support the correct use of JORA, review quality, efficiency and user-satisfaction of the system in accordance with the needs.

The JORA Product and Service Management is responsible for the following tasks:

- To coordinate and carry out the activities required in order to ensure the daily operational management of the system;
- To communicate with external customers and Frontex entities;
- To manage and maintain the Service-Level Agreement with Frontex ICT;
- To manage the content and the structural design of the application;
- To manage the Requests for Change;
- To identify and assess the training needs, and to plan, coordinate, organize and deliver the relevant training activities, where possible;
- To report risks, statistics and issues to the Business Owner;
- To initiate and coordinate the execution of new developments;
- To provide their expertise to new activities related to the product development;
- To initiate quality checks.

In order to maintain the required operational support, the JORA Product and Service Management provides daily expertise, consultancy and assistance to its stakeholders and customers.

Suggestions and feedback are part of the adopted Continual Service Improvement orientation. Thus, the JORA Product and Service Management welcomes any feedback received from the end users: suggestions, recommendations and Requests for Change are assessed and analysed.

10.1.2. JORA Roles and Responsibilities

All assigned JORA actors are listed in the respective Specific Annex of the Operational Plan.

10.1.2.1.JORA Administrator

- Staff member nominated by the Head of the Frontex Situation Centre ;
- Authorized to manage all the roles and processes in JORA;
- May define, modify and delete operations in JORA;

10.1.2.2.JORA Frontex Access Manager

- Operational Manager of the joint operation;
- Creates the operation and its structure in the JORA system according to the Operational Plan;
- Selects and assigns the incident template creator in the JORA system, and approves the relevant incident template;

Commented [KW34]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

- Manages the operational access requests coming from members of the EU Institutions, from Frontex, and from other authorities who take part to the operation;
- Manages the operational access requests coming from members of the EU Institutions, from Frontex, and from other authorities when the National Authority box is checked in the Operational access request
- Assigns and manages the Operational National Access Managers appointed to the operation in the JORA system;
- Selects delegated Operational Manager(s) in the system when a new operation is created;
- Acts as the Incident Template Verifier;
- Manages users concerning this operation.

10.1.2.3.JORA Delegated Project Manager

The same set of responsibilities applies as to JORA Frontex Access Manager.

10.1.2.4.FSC Support Officers

The FSC delivers the necessary training for JORA, in accordance with the role and the responsibility of the Support Officers.

FSC ensures that all the support officers having appropriate user rights in the JORA system to perform their tasks during their deployment.

10.1.2.5.JORA National Access Manager

National Access Managers are nominated by their MS / National Authorities.

Responsibilities:

- To approve or reject the Initial Access Requests from member of national entities participating in Frontex joint operations and other activities to define the operational access rights;
- To manage the users' accounts for the operation.

10.1.2.6.JORA Operational National Access Manager

Operational National Access Managers are assigned by Frontex Access Manager for each operation.

Responsibilities:

- To define the operational access rights;
- To manage the users' accounts for the operation.

10.1.2.7.JORA Incident Reporter

Host MS officer(s) or deployed officer(s) are responsible for the incident reporting depending on the organization of the daily operational activities. In case deployed officers are involved in the incident reporting working flow it is strongly advised that the host country authorities appoint a local officer for the coordination of the incident reporting in the JORA system (such as incident verifier).

The incident reporters' main responsibilities are to create, modify, and forward incident reports to the next validation level, in accordance with the Operational Plan.